



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/617,069

07/10/2003

Shinako Matsuyama

112857-411

3783

29175 7590 05/10/2007
BELL, BOYD & LLOYD, LLP
P. O. BOX 1135
CHICAGO, IL 60690

EXAMINER

SMARTH, GERALD A

ART UNIT

PAPER NUMBER

2109

MAIL DATE

DELIVERY MODE

05/10/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.		Applicant(s)	
	10/617,069		MATSUYAMA, SHINAKO	
	Examiner		Art Unit	
	Gerald Smarth		2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 1-13 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-13 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|--|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>10/07/03</u> . | 6) <input type="checkbox"/> Other: ____ |

DETAILED ACTION

Title

The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

Claim Rejections - 35 USC § 112

1. Claim 5 & 11 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 5 states a remote access system according to claim 4, wherein the certificate in which access privilege with regard to the resource is described includes information indicating that permission to issue to the accessing unit the certificate in which access privilege with regard to the resource is described is given, as role information indicating a role assigned to the connection unit.

The role information is explained briefly and it is not understood how it correlates with present invention.

Art Unit: 2109

Claim 11 a remote access method according to claim 10, wherein the certificate in which access privilege with regard to the resource is described includes information indicating that permission to issue to the accessing unit the certificate in which access privilege with regard to the resource is described is given, as role information indicating a role assigned to the connection unit.

The role information is explained briefly and it is not understood how it correlates with present invention.

Claim Rejections - 35 USC § 102

1. Claims 1-13 rejected under 35 U.S.C. 102(b) as being anticipated by Baize(6317838)

Claim 1 states a remote access system for accessing a predetermined resource from a remote place, comprising: an access target unit to be accessed(Fig. Wk1, Wkx, Wka); (Baize discloses "The invention concerns a method to provide a secured remote access to private resources." Column 1 line 7)

An accessing unit (fig 1-2) for accessing the access target unit; and a connection unit(fig 1 SS) for standing proxy for the access target unit to the accessing unit, wherein the accessing unit comprises: storage means(fig 1 DBs) for storing a certificate(fig 4a. 820) in which access privilege with regard to the resource is described; (Baize discloses "Implementing in said digital data processing system security storing means for storing security data, said security data comprising at least data to authenticate said user,

Art Unit: 2109

security profiles indicating which private resources each user may use and security data associated with said private resources. column 4 line 25)

Presenting means for presenting the certificate stored in the storage means to the access target unit having the resource, the connection unit comprises: (Baize discloses "at the user's side, a first stage comprising the opening of a session, a second stage comprising the entering of security data, including at least user's authentication data, and a third stage of requesting an access to a first private resource. Column 4 line 38)

Verification means for verifying the certificate received from the accessing unit; and transmission means for transmitting the certificate verified by the verification means to the access target unit specified by the accessing unit, (Baize discloses "A dialog is initiated between the security server Ss and this piece of security software 6, via a bus 60. The data transmissions are enciphered. The server Ss looks at the data base DBs and compares the received data(identity of user U1, password, etc.) with the content of said data base Dbs. It authenticates the requester, i.e. user U1, and send back a message to workstation WK1 and more precisely to it's security interface." column 5 line 41)

The access target unit comprises determination means for determining according to the certificate transmitted by the connection unit whether to permit the accessing unit to access the resource. (Baize discloses "When a user or a client device attempts to access to a particular protected resource located in a data processing system, generally it is necessary to check whether it may or not access to said resource. For example if

Art Unit: 2109

the user sends a request so as to read some protected data, its request must be filtered, before granting such an access. On the second hand, after this authentication stage is performed, the request is allowed or discarded according to his rights or privileges." Column 1 line 23)

Claim 2 states a remote access system according to claim 1, where in the connection unit connects a network which includes the access target unit and another network to each other. (Baize discloses "The first solution is know as a "VPN"(Virtual Private Network"). It consists in providing secured " data pipes" constituting so-called "Extranets" which are extensions of Intranets or LANs. " VPNs can connect from one network to another. "Column 3 line 3)

Claim 3 states a remote access system according to claim 1, wherein the certificate includes proxy information which indicates that the connection unit stands proxy for the access target unit. (Baize discloses" A typical proxy accepts a connection, makes a decision on whether or not the user or the client IP address is permitted to use the proxy(according to the requested server or resource, time period , etc.), possibly does additional authentication , and completes a connection on behalf of the user to the remote server or resource, through bus Bo(output bus)"column 6 line 36).

Claim 4 states a remote access system according to claim 1, further comprising an authority for issuing an issue permission certificate serving as a certificate for giving permission to issue to the accessing unit, the certificate in which access privilege with regard to the resource is described, wherein the connection unit issues the issue permission certificate issued by the authority, to the accessing unit. (Baize discloses " A

Art Unit: 2109

security server Ss is also provided. It communicates with a security data base DBs which contains security and authorization profiles of both secured or private resources, ie S1 to Sm, and local users, for example U1. The security server Ss is supposed to be under control of a security officer" column 5 line 27)

Claim 6 states a remote access system according to claim 1, further comprising a certificate authority for issuing a public-key certificate based on a public-key cryptosystem, to each entity constituting the remote access system. (Baize discloses "On networks of the "VPN" type solution commonly uses low-level algorithms or weak keys, which is not sufficient to protect very sensitive data, as passwords for example". Column 3 line 19)

Claim 7 states a remote access method for accessing a predetermined resource from a remote place, comprising: a storage step of storing a certificate in which access privilege with regard to the resource is described; a presenting step of presenting the certificate stored in the storage step to an access target unit having the resource; (Baize discloses "Implementing in said digital data processing system security storing means for storing security data, said security data comprising at least data to authenticate said user, security profiles indicating which private resources each user may use and security data associated with said private resource" Column 4 line 26)

A verification step of verifying the certificate received from an accessing unit for accessing the access target unit; a transmission step of transmitting the certificate verified in the verification step to the access target unit specified by the accessing unit; and a determination step of determining whether to permit the accessing unit to access

Art Unit: 2109

the resource, according to the certificate transmitted by a connection unit for standing proxy for the access target unit to the accessing unit. (Baize discloses "A dialog is initiated between the security server Ss and this piece of security software 6, via a bus 60. The data transmissions are enciphered. The server Ss looks at the data base DBs and compares the received data(identity of user U1, password, etc.) with the content of said data base Dbs. It authenticates the requester, i.e. user U1, and send back a message to workstation WK1 and more precisely to it's security interface." column 5 line 41)

Claim 8 states a remote access method according to claim 7, wherein a network which includes the access target unit and another network are connected to each other. (Baize discloses " The first solution is know as a "VPN"(Virtual Private Network)". It consists in providing secured " data pipes" constituting so-called "Extranets" which are extensions of Intranets or LANs. " VPNs can connect from one network to another. Column 3 page 3)

Claim 9 states a remote access method according to claim 7, wherein the certificate includes proxy information which indicates that the connection unit stands proxy for the access target unit. (Baize discloses" A typical proxy accepts a connection, makes a decision on whether or not the user or the client IP address is permitted to use the proxy(according to the requested server or resource, time period , etc.), possibly does additional authentication , and completes a connection on behalf of the user to the remote server or resource, through bus Bo(output bus)column 6 line 36).

Claim 10 states a remote access method according to claim 7, further comprising a step of issuing an issue permission certificate serving as a certificate for giving permission to issue to the accessing unit, the certificate in which access privilege with regard to the resource is described, wherein the issue permission certificate issued by the authority is issued to the accessing unit. (Blaize discloses " A security server Ss is also provided. It communicates with a security data base DBs which contains security and authorization profiles of both secured or private resources, ie S1 to Sm, and local users, for example U1. The security server Ss is supposed to be under control of a security officer" column 5 line 27)

Claim 12 states a remote access method according to claim 7, further comprising a step of issuing a public-key certificate based on a public-key cryptosystem, to each entity constituting the remote access method. (Blaize discloses " On networks of the "VPN" type solution commonly uses low-level algorithms or weak keys, which is not sufficient to protect very sensitive data, as passwords for example" column 3 line 19)

Claim 13 States a remote access program executable by a computer, for accessing a predetermined resource from a remote place, the program comprising: a storage step of storing a certificate in which access privilege with regard to the resource is described; a presenting step of presenting the certificate stored in the storage step to an access target unit having the resource; (Baize discloses "Implementing in said digital data processing system security storing means for storing security data, said security data comprising at least data to authenticate said user, security profiles indicating which

Art Unit: 2109

private resources each user may use and security data associated with said private resource" Column 4 line 26)


A verification step of verifying the certificate received from an accessing unit for accessing the access target unit; a transmission step of transmitting the certificate verified in the verification step to the access target unit specified by the accessing unit; and a determination step of determining whether to permit the accessing unit to access the resource, according to the certificate transmitted by a connection unit for standing proxy for the access target unit to the accessing unit. ,(Baize states "A dialog is initiated between the security server Ss and this piece of security software 6, via a bus 60. The data transmissions are enciphered. The server Ss looks at the data base DBs and compares the received data(identity of user U1, password, etc.) with the content of said data base Dbs. It authenticates the requester, i.e. user U1, and send back a message to workstation WK1 and more precisely to it's security interface." column 5 line 41)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Gerald Smarth whose telephone number is (571)270-1923. The examiner can normally be reached on Monday-Friday(7:30am-5:00pm)est.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeff Pwu can be reached on (571)272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2109

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



JEFFREY PWU
SUPERVISORY PATENT EXAMINER